U.S. Department of Justice

Stephen J. Murphy
United States Attorney
Eastern District of Michigan

Suite 2001
211 West Fort Street
Detroit, Michigan 48226-3277
Fax: (313) 226-3561

For Immediate Release:
Contact: Gina Balaya (313) 226-9758

Oct 23, 2007

EVENT: Sentencing

Defendant: Jason Michael Downey

OPERATOR OF "BOT-NET", A NETWORK
OF THOUSANDS OF VIRUS-INFECTED COMPUTERS,
SENTENCED TO 12 MONTHS IN FEDERAL PRISON

Jason Michael Downey, the operator of "bot network" of virus infected computers that he used to attack other computer systems, was sentenced to a year in federal prison today on his conviction for unlawful computer intrusion that caused over $20,000 in damages to other computer networks, United States Attorney Stephen J. Murphy announced today.

Murphy was joined in the announcement by Andrew G. Arena, FBI Special Agent in Charge.

Jason Michael Downey, 24, of Dry Ridge, Kentucky, was sentenced by United States District Judge Nancy G. Edmunds to 12 months' custody in the Bureau of Prisons, 3 years' supervised release, and ordered to pay $21,110 in restitution to the three victim computer networks, and perform 150 hours of community service during the period of supervised release, as well as to pay a $100 special assessment.

At sentencing, Judge Edmunds noted that computer crime inflicted serious damages on society and that the crime deserved a serious punishment. Information presented to the court at the time of the sentence showed that from on or about June 18, 2004 through on or about September 5, 2004, Defendant was the owner of the Rizon.net Internet Relay Chat (or “IRC”) network. During that time defendant operated a "bot-network," that is, a network of computers infected with a virus that allowed defendant to control such computers, and cause them to attack other computers by sending high volumes of data to such target computers, and thereby causing damage by impairing the availability of such systems. In particular, Defendant caused a large number of computers to be infected with several kinds of "bot" viruses that would cause such computers to respond to commands that defendant issued. As a result, Defendant created a network of infected computers, or "bot-net," of up to 6,000 infected computers. An unspecified number of the infected computers were in the Eastern District of Michigan. Thereafter, Defendant used the Internet Relay Chat network known as "Yotta-byte.net" to control and send commands to the bot-net in order to launch "denial of service" attacks on a variety of computer systems on the Internet, causing such systems to be overloaded with network data and unable to function properly and thereby impairing the operability of such systems. The losses caused by this conduct were over $20,000.

United States Attorney Stephen J. Murphy said, “The so-called ‘bot-masters’ on the Internet should realize that attacking and damaging other computer networks through a bot-net can land you in prison. We have the capacity to investigate and prosecute these high tech crimes and we will continue to do so. I commend the FBI for the excellent investigative work they did in this case.”

The case was prosecuted by First Assistant United States Attorney Terrence Berg.